REPORT DOCUMENTATION PAGE

Form Approved
OMB NO. 0704-0188

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	31 Mar 98	TECHNICAL

4. TITLE AND SUBTITLE

HYBRID SYSTEMS WITH FINITE BISIMULATIONS

5. FUNDING NUMBERS

DAAH04-95-1-0588

6. AUTHOR(S)

G. LAFFERRIERE, G. PAPPAS, and S. SASTRY

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Regents of the University of California
c/o Sponsored Projects Office
336 Sproul Hall
Berkeley, CA 94720-5940

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U. S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

ARO 34811.14-MS

11. SUPPLEMENTARY NOTES

The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision, unless so designated by the documentation.

12 a. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution unlimited.

12 b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

ABSTRACT. The theory of formal verification is one of the main approaches to hybrid system analysis. A unified approach to decidability questions for verification algorithms is obtained by the construction of a bisimulation. Bisimulations are finite state quotients whose reachability properties are equivalent to those of the original infinite state hybrid system. This approach has had success in the reachability analysis of timed automata and initialized rectangular automata. In this paper, we use recent results from stratification theory, subanalytic sets, and model theory in order to extend the state-of-the-art results on the existence of bisimulations for certain classes of hybrid systems.

14. SUBJECT TERMS

HYBRID SYSTEMS, BISIMULATIONS, SUBANALYTIC SETS, STRATIFICATION

15. NUMBER OF PAGES

18

16. PRICE CODE

17. SECURITY CLASSIFICATION OR REPORT	18. SECURITY CLASSIFICATION ON THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev.2-89)
Prescribed by ANSI Std. 239-18
298-102

Technical Report *UCB/ERL M98/15*, University of California at Berkeley, April 1998

HYBRID SYSTEMS WITH FINITE BISIMULATIONS

GERARDO LAFFERRIERE, GEORGE J. PAPPAS, AND SHANKAR SASTRY

ABSTRACT. The theory of formal verification is one of the main approaches to hybrid system analysis. A unified approach to decidability questions for verification algorithms is obtained by the construction of a bisimulation. Bisimulations are finite state quotients whose reachability properties are equivalent to those of the original infinite state hybrid system. This approach has had success in the reachability analysis of timed automata and initialized rectangular automata. In this paper, we use recent results from stratification theory, subanalytic sets, and model theory in order to extend the state-of-the-art results on the existence of bisimulations for certain classes of hybrid systems.

1. INTRODUCTION

Hybrid systems consist of finite state machines interacting with differential equations. Various modeling formalisms, analysis, design and control methodologies, as well as applications, can be found in [2, 3, 4, 10, 16]. The theory of formal verification is one of the main approaches for analyzing properties of hybrid systems. The system to be analyzed is first modeled as a hybrid automaton, and the desired property is expressed using a formula from some temporal logic. Then, model checking or deductive algorithms are used in order to guarantee that the system model indeed satisfies the desired property.

Verification algorithms are essentially reachability algorithms which check whether trajectories of the hybrid system can reach certain undesirable regions of the state space. Since hybrid systems have infinite state spaces, decidability of verification algorithms is very important. Decidability results for analyzing hybrid systems consider special finite state quotients of the original infinite state hybrid automaton called *bisimulations*. Bisimulations are reachability preserving quotient systems in the sense that checking a property on the quotient system is *equivalent* to checking the property on the original system. Showing that an infinite state hybrid automaton has a finite state bisimulation is the first step in proving that verification procedures are decidable. This approach has yielded several classes of decidable hybrid systems including timed automata [1], initialized rectangular automata [20], and linear hybrid automata [11]. Some undecidable classes have also been discovered in [12]. Computing finite bisimulations is clearly related to the problem of obtaining discrete abstractions of continuous systems which has been considered by [21, 17, 5] as well as [8].

Since the discrete dynamics are already finite, it is clear that decidability results for hybrid systems depend crucially on the success of obtaining finite bisimulations for continuous dynamics. The cases considered so far in the literature dealt with simple dynamics: $\dot{x} = 1$ for timed automata [1], $\dot{x} \in [a, b]$ for rectangular automata [20], and $A\dot{x} \leq b$ for linear hybrid automata [11]. In this paper, we extend the bisimulation methodology to hybrid systems

with more general dynamics. We describe an algorithm which, upon termination, provides the desired finite bismilarity quotient. In order to investigate classes of systems for which the algorithm terminates, we combine mathematical techniques from differential geometry and recent results in logic model theory. With these new tools, we prove the existence of finite bisimulations for various classes of hybrid systems with planar continuous dynamics. This convergence of mathematical logic and differential geometry also provides a natural framework for extending the decidability frontier for more general classes of hybrid systems. Such extensions will require pushing the boundary of decidable theories in mathematical logic.

Abstracting a discrete graph from a hybrid system requires the analysis of trajectories of vector fields and their intersection properties relative to a given collection of sets. Considering hybrid systems with arbitrary dynamics and arbitrary state partitions would soon lead to pathological situations. *Subanalytic sets* [6, 13, 23] provide a rich class of sets which have many desirable local intersection properties with trajectories of *analytic* vector fields. Subanalytic sets can also be partitioned into smooth embedded submanifolds in a form suitable for constructing a bisimulation. Such partitions are called *stratifications*. Moreover, we show that relaxing the class of vector fields or sets in some naive ways leads to pathological situations. On the other hand, the concept of *o-minimal* theories in logic [26, 27, 28] identifies classes of sets with good intersection properties suitable for the global study of trajectories of vector fields. The combination of techniques from both fields highlights the kind of properties of sets that play a central role in obtaining discrete abstractions.

The outline of the paper is as follows: In Section 2 we review the notion of bisimulations of transitions systems. In Section 3 we define the class of hybrid systems under study and describe the main algorithm of the paper (**Algorithm 2**). Section 4 presents some basic facts about stratification theory and subanalytic sets and relates them to the construction of bisimulations. In Section 5 we present recent results in model theory which are used in Section 6 in order to obtain classes of systems for which the bisimulation algorithm terminates. Section 7 contains conclusions and issues for further research.

2. Bisimulations of Transition Systems

We adopt here the terminology of [11] slightly modified for our purposes. A transition system $T = (Q, \Sigma, \rightarrow, Q_O, Q_F)$ consists of a (not necessarily finite) set Q of states, an alphabet Σ of events, a transition relation $\rightarrow \subseteq Q \times \Sigma \times Q$, a set $Q_O \subseteq Q$ of initial states, and a set $Q_F \subseteq Q$ of final states. A transition $(q_1, \sigma, q_2) \in \rightarrow$ is denoted as $q_1 \xrightarrow{\sigma} q_2$. The transition system is finite if the cardinality of Q is finite and it is infinite otherwise. A region is a subset $P \subseteq Q$. Given $\sigma \in \Sigma$ we define the predecessor $Pre_\sigma(P)$ of a region P as

$$Pre_\sigma(P) = \{q \in Q \mid \exists p \in P \text{ and } q \xrightarrow{\sigma} p\} \tag{2.1}$$

Given an equivalence relation $\sim \subseteq Q \times Q$ on the state space one can define a quotient transition system as follows. Let $Q/\sim$ denote the quotient space. For a region P we denote by $P/\sim$ the collection of all equivalence classes which intersect P. The transition relation $\rightarrow_\sim$ on the quotient space is defined as follows: for $Q_1, Q_2 \in Q/\sim$, $Q_1 \xrightarrow{\sigma}_\sim Q_2$ iff there exist

$q_1 \in Q_1$ and $q_2 \in Q_2$ such that $q_1 \xrightarrow{\sigma} q_2$. The quotient transition system is then $T/\sim = (Q/\sim, \Sigma, \rightarrow_\sim, Q_0/\sim, Q_F/\sim)$.

Given an equivalence relation $\sim$ on Q, we call a set a $\sim$-block if it is a union of equivalence classes. The equivalence relation $\sim$ is a *bisimulation* of T iff Q_O, Q_F are $\sim$-blocks and for all $\sigma \in \Sigma$ and all $\sim$-blocks P, the region $Pre_\sigma(P)$ is a $\sim$-block. In this case the systems T and $T/\sim$ are called *bisimilar*. We will also say that a partition is a bisimulation when its induced equivalence relation is a bisimulation. A bisimulation is called finite if it has a finite number of equivalence classes. Bisimulations are very important because bisimilar transition systems generate the same language [11]. Therefore, checking properties on the bisimilar transition system is equivalent to checking properties of the original transition system. This is very useful in reducing the complexity of various verification algorithms where Q is finite but very large. In addition, if T is infinite and $T/\sim$ is a finite bisimulation, then verification algorithms for infinite systems are guaranteed to terminate. Successful applications of this approach for hybrid systems include timed automata [1], initialized rectangular automata [20], and linear hybrid automata [11]. It should be noted that the notion of bisimulation is similar to the notion of dynamic consistency [7, 8, 18]. If $\sim$ is a bisimulation, it can be easily shown that if $p \sim q$ then

B1: $p \in Q_F$ iff $q \in Q_F$, and $p \in Q_O$ iff $q \in Q_O$
B2: if $p \xrightarrow{\sigma} p'$ then there exists q' such that $q \xrightarrow{\sigma} q'$ and $p' \sim q'$

Based on the above characterization, given a transition system T, the following algorithm computes increasingly finer partitions of the state space Q. If the algorithm terminates, then the resulting quotient transition system is a finite bisimulation. The state space $Q/\sim$ is called a bisimilarity quotient.

Algorithm 1: (Bisimulation Algorithm for Transition Systems)
Set: $Q/\sim = \{Q_O \cap Q_F, Q_O \setminus Q_F, Q_F \setminus Q_O, Q \setminus (Q_O \cup Q_F)\}$
while: $\exists\ P, P' \in Q/\sim$ and $\sigma \in \Sigma$ such that $\emptyset \neq P \cap Pre_\sigma(P') \neq P$
  set: $P_1 = P \cap Pre_\sigma(P')$, $P_2 = P \setminus Pre_\sigma(P')$
  refine: $Q/\sim = (Q/\sim \setminus \{P\}) \cup \{P_1, P_2\}$
end while:

Notice that each time the partition $Q/\sim$ is refined, the transitions are updated to account for the newly subdivided sets. When checking specific properties, such as reachability to the set Q_F, one might simplify the algorithm by starting with a coarser partition, for example $\{Q_F, Q \setminus Q_F\}$. In general one should include in the initial partition all additional sets relevant to the verification problem of interest (such as safe or unsafe regions). The larger the initial class of sets the more difficult it is for the algorithm to terminate.

3. Bisimulations of Hybrid Systems

We focus on transition systems generated by the following class of hybrid systems.

Definition 3.1. A *hybrid system* is a tuple $H = (X, X_0, X_F, F, E, I, G, R)$ where

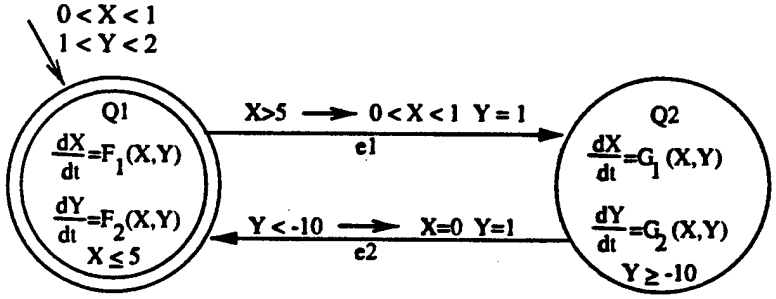

FIGURE 1. A typical hybrid automaton

- $X = X_D \times X_C$ is the state space with $X_D = \{q_1, \ldots, q_n\}$ and X_C an analytic manifold.
- $X_0 \subseteq X$ is the set of initial states
- $X_F \subseteq X$ is the set of final states
- $F : X \longrightarrow TX_C$ assigns to each discrete state $q \in X_D$ an analytic vector field $F(q, \cdot)$
- $E \subseteq X_D \times X_D$ is the set of discrete transitions
- $I : X_D \longrightarrow 2^{X_C}$ assigns to each discrete state a set $I(q) \subseteq X_C$ called the invariant.
- $G : E \longrightarrow X_D \times 2^{X_C}$ assigns to $e = (q_1, q_2) \in E$ a guard of the form $\{q_1\} \times U$, $U \subseteq I(q_1)$.
- $R : E \longrightarrow X_D \times 2^{X_C}$ assigns to $e = (q_1, q_2) \in E$ a reset of the form $\{q_2\} \times V$, $V \subseteq I(q_2)$.

Trajectories of the hybrid system H originate at any $(q, x) \in X_0$ and consist of either continuous evolutions or discrete jumps. Continuous trajectories keep the discrete part of the state constant, and the continuous part evolves according to the continuous flow $F(q, \cdot)$ as long as the flow remains inside the invariant set $I(q)$. If the flow exits $I(q)$, then a discrete transition is *forced*. If, during the continuous evolution, a state $(q, x) \in G(e)$ is reached for some $e \in E$, then discrete transition e is *enabled*. The hybrid system may then instantaneously jump from (q, x) to any $(q', x') \in R(e)$ and the system then evolves according to the flow $F(q', \cdot)$. Notice that even though the continuous evolution is deterministic, the discrete evolution may be nondeterministic. The discrete transitions allowed in our model are of the type allowed in initialized rectangular automata [20]. We assume that our hybrid system model is *non-blocking*, that is from every state either a continuous evolution or a discrete transition is possible.

Example 3.2. A typical hybrid system is shown in Figure 1. The state space is $\{Q1, Q2\} \times \mathbb{R}^2$. The initial states are of the form $\{Q1\} \times \{(x, y) \in \mathbb{R}^2 \mid 0 < x < 1, 1 < y < 2\}$. The discrete dynamics consists of two transitions $e_1 = (Q1, Q2)$ and $e_2 = (Q2, Q1)$. Within discrete state $Q1$, the continuous variables x and y evolve according to a differential equation as long as $(x, y) \in I(Q_1) = \{(x, y) \in \mathbb{R}^2 \mid x \leq 5\}$. Once $x > 5$, discrete transition e_1 is forced and x,y are nondeterministically reset to values in fixed sets. The system then flows according to the flow associated with $Q2$. The evolution from that point on is similar. We would like to find out whether the system will reach the set of final states $\{Q_2\} \times \{(x, y) \in \mathbb{R}^2 \mid x < -5\}$.

Every hybrid system $H = (X, X_0, X_F, F, E, I, G, R)$ generates a transition system $T = (Q, \Sigma, \rightarrow, Q_O, Q_F)$ by setting $Q = X$, $Q_0 = X_0$, $Q_F = X_F$, $\Sigma = E \cup \{\tau\}$, and $\rightarrow = (\cup_{e \in E} \xrightarrow{e}) \cup \xrightarrow{\tau}$ where

Discrete Transitions: $(q, x) \xrightarrow{e} (q', x')$ for $e \in E$ iff $(q, x) \in G(e)$ and $(q', x') \in R(e)$

Continuous Transitions: $(q_1, x_1) \xrightarrow{\tau} (q_2, x_2)$ iff $q_1 = q_2$ and there exists $\delta \geq 0$ and a curve $x : [0, \delta] \longrightarrow M$ with $x(0) = x_1$, $x(\delta) = x_2$ and for all $t \in [0, \delta]$ it satisfies $x' = F(q_1, x(t))$ and $x(t) \in I(q_1)$.

The continuous τ transitions are time-abstract transitions, in the sense that the time it takes to reach one state from another is ignored. Having defined the continuous and discrete transitions $\xrightarrow{\tau}$ and $\xrightarrow{e}$ allows us to formally define $Pre_\tau(P)$ and $Pre_e(P)$ for $e \in E$ and any region $P \subseteq X$ using (2.1). Furthermore, the structure of the discrete transitions allowed in our hybrid system model result in

$$Pre_e(P) = \begin{cases} \emptyset & \text{if } P \cap R(e) = \emptyset \\ G(e) & \text{if } P \cap R(e) \neq \emptyset \end{cases} \tag{3.1}$$

for all discrete transitions $e \in E$ and regions P. Therefore, if the sets $R(e)$ and $G(e)$ are blocks of any partition of the state space, then no partition refinement is necessary in the bisimulation algorithm due to any discrete transitions $e \in E$. This fact, in a sense, decouples the continuous and discrete components of the hybrid system. In turn, this implies that the initial partition in the bisimulation algorithm should contain the invariants, guards and reset sets, in addition to the initial and final sets. This allows us to carry out the algorithm independently for each discrete state.

More precisely, define for any region $P \subseteq X$ and $q \in X_D$ the set $P_q = \{x \in X_C : (q, x) \in P\}$. For each discrete state $q \in X_D$ consider the finite collection of sets

$$\mathcal{A}_q = \{I(q), G(e)_q, R(e)_q, (X_0)_q, (X_F)_q\} \tag{3.2}$$

which describes the initial and final states, guards, invariants and resets associated with discrete state q. Let $\mathcal{S}_q$ be the coarsest partition of X_C compatible with the collection $\mathcal{A}_q$ (by compatible we mean that each set in $\mathcal{A}_q$ is a union of sets in $\mathcal{S}_q$). The (finite) partition $\mathcal{S}_q$ can be easily computed by successively finding the intersections between each of the sets in $\mathcal{A}_q$ and their complements. These collections $\mathcal{S}_q$ will be the starting partitions of the bisimulation algorithm.

Algorithm 2: (Bisimulation Algorithm for Hybrid Systems)
Set: $X/\sim \; = \bigcup_q \mathcal{S}_q$
for: $q \in X_D$
  while: $\exists\, P, P' \in \mathcal{S}_q$ such that $\emptyset \neq P \cap Pre_\tau(P') \neq P$
    Set: $P_1 = P \cap Pre_\tau(P')$; $P_2 = P \setminus Pre_\tau(P')$
    refine: $\mathcal{S}_q \; = (\mathcal{S}_q \setminus \{P\}) \cup \{P_1, P_2\}$
  end while:
end for:

A few comments are in order here. The key problem is to investigate how the flow of $F(q, \cdot)$ interacts with the sets $\mathcal{S}_q$ for a single discrete state q. This requires that the trajectories of the vector field $F(q, \cdot)$ have "nice" intersection properties with such sets. Since the goal is to obtain finite partitions, it will become important that we restrict the study to classes of sets with good "finiteness" properties, for example, sets with finitely many connected components. In the

subsequent sections we identify classes of sets and vector fields which exhibit such properties and for which **Algorithm 2** terminates.

One can also view the partitions in the algorithm as a way of discretizing the system trajectories. This suggests studying the continuous transitions by looking only at the points at which the trajectories move from one set in $\mathcal{S}_q$ to an "adjacent" one. This is in general not possible because sets could have rather pathological boundaries (see also Example 4.8). We will see in the next section that subanalytic sets are free from such pathologies and that in fact one can formalize the idea of trajectory discretization associated to the partition in that case.

We conclude this section with an example that shows that, even in apparently simple situations, **Algorithm 2** does not terminate.

Example 3.3. Let F be the linear vector field $\begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix} \mathbf{x}$ on $\mathbb{R}^2$. Assume the partition of $\mathbb{R}^2$ consists of the following three sets (see Figure 2): $P_1 = \{(x,0) : 0 \leq x \leq 4\}$, $P_2 = \{(x,0) : -4 \leq x < 0\}$, $P_3 = \mathbb{R}^2 \setminus (P_1 \cup P_2)$. The integral curves of F are spirals moving away

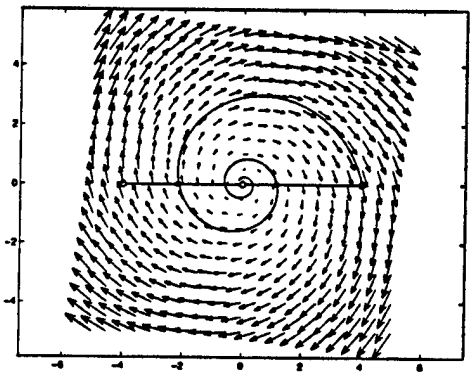

FIGURE 2. Algorithm 2 does not terminate

from the origin. The first iteration of the algorithm partitions P_2 into $P_4 = P_2 \cap Pre_\tau(P_1) = \{(x,0) : x_1 \leq x < 0\}$ and $P_2 \setminus Pre_\tau(P_1)$. Here $x_1 < 0$ is the x-coordinate of the first intersection point of the spiral through $(4,0)$ with P_2. The second iteration subdivides P_1 into $P_5 = P_1 \cap Pre_\tau(P_4) = \{(x,0) : 0 \leq x \leq x_2\}$ and $P_1 \setminus Pre_\tau(P_4)$ where $x_2 > 0$ is the x-coordinate of the next point of intersection of the spiral with P_1. This process continues indefinitely since the spiral intersects P_1 in infinitely many points, and therefore the algorithm does not terminate.

4. SUBANALYTIC SETS AND STRATIFICATIONS

In this section we describe some fundamental properties of *subanalytic sets* (see [6, 13, 23] for more details). A differentiable manifold is *real analytic* (C^ω) if the transition maps between local coordinate charts are analytic functions on their domains (which are open subsets of $\mathbb{R}^n$). An *embedded submanifold* S of a manifold M is a topological subspace of M together with a

differentiable structure such that the inclusion from S into M is a smooth immersion (i.e. has full rank at every point). A vector field F on the real analytic manifold M is *analytic* if its coordinates in any local chart are analytic. If F is an analytic vector field then any integral curve of F is analytic.

Let M and N be real analytic manifolds and let $C^\omega(M,N)$ denote the set of analytic functions from M into N. If $f \in C^\omega(M,N)$ we say f is of class C^ω. Given an analytic manifold U, we denote by $\Sigma(C^\omega(U,\mathbb{R}))$ the Boolean algebra generated by the sets of the form $\{x : f(x) = 0\}$ or $\{x : f(x) > 0\}$, where $f \in C^\omega(U,\mathbb{R})$.

Definition 4.1. Let M be a real analytic manifold. A subset A of M is *semianalytic in* M if for every $p \in M$, there is an open neighborhood U of p in M such that $U \cap A \in \Sigma(C^\omega(U,\mathbb{R}))$. If $A \subseteq M$ is semianalytic in M we write $A \in \mathrm{SMAN}(M)$.

Definition 4.2. Let M be a real analytic manifold. Define $\mathrm{SBAN}_{rc}(M)$ and $\mathrm{SBAN}(M)$ by

1. $A \in \mathrm{SBAN}_{rc}(M)$ if and only if there is (N, f, A^*) such that N is a real analytic manifold, $f \in C^\omega(N,M)$, $A^* \in \mathrm{SMAN}(N)$, A^* is relatively compact and $A = f(A^*)$;
2. $A \in \mathrm{SBAN}(M)$ if and only if A is the union of a locally finite collection of members of $\mathrm{SBAN}_{rc}(M)$. (A collection of sets $\mathcal{C}$ is locally finite if any compact set intersect only finitely many sets in $\mathcal{C}$.)

We say that A is *subanalytic in* M if $A \in \mathrm{SBAN}(M)$. It is easy to see that $A \in \mathrm{SBAN}_{rc}(M)$ if and only if A is subanalytic in M and relatively compact. The following properties of subanalytic sets are easily derived from the definitions.

1. $\mathrm{SBAN}(M)$ is closed under locally finite unions and intersections.
2. If $A \in \mathrm{SBAN}(M)$ and $f\colon M \longrightarrow N$ is of class C^ω and proper on $\overline{A}$, the closure of A, then $f(A) \in \mathrm{SBAN}(N)$. (A function f is *proper* if $f^{-1}(K)$ is compact whenever K is.)
3. If $A \in \mathrm{SBAN}(N)$ and $f\colon M \longrightarrow N$ is of class C^ω, then $f^{-1}(A) \in \mathrm{SBAN}(M)$.

The following two properties require more subtle proofs, but they give the first indication that this will be a suitable class of sets for our studies.

4. If $A \in \mathrm{SBAN}(M)$ then $M \setminus A \in \mathrm{SBAN}(M)$.
5. A subanalytic set has a locally finite number of connected components, each of which is subanalytic.

Example 4.3. Points are subanalytic, and so is any locally finite union of points, for example $\mathbb{Z}^n$ as subset of $\mathbb{R}^n$. The empty set and M are both in $\mathrm{SBAN}(M)$. Let $a, b \in \mathbb{R}$, $a < b$, then $[a,b]$, $[a,b)$, $(a,b]$ and (a,b) are subanalytic in $\mathbb{R}$. The open ball $B(p,r)$ centered at p of radius r in $\mathbb{R}^n$ is in $\mathrm{SBAN}(\mathbb{R}^n)$.

Definition 4.4. Let M be a real analytic manifold. An *analytic (C^ω) stratification* of M is a partition $\mathcal{S}$ of M with the following properties:

1. each $S \in \mathcal{S}$ is a connected, real analytic, embedded submanifold of M,
2. $\mathcal{S}$ is locally finite,
3. given two sets $S, P \in \mathcal{S}$, $P \neq S$, such that $S \cap \overline{P} \neq \emptyset$ then $S \subset \overline{P}$ and $\dim S < \dim P$.

The sets in a stratification are called *strata.*

The central result on stratifications for our analysis is the following. For a proof see [22].

Theorem 4.5. *Let $\mathcal{A}$ be a locally finite family of nonempty subanalytic subsets of a real analytic manifold M. For each $A \in \mathcal{A}$, let $F(A)$ be a finite set of real analytic vector fields on M. Then there exists a subanalytic stratification $\mathcal{S}$ of M, compatible with $\mathcal{A}$, and having the property that, whenever $S \in \mathcal{S}$, $S \subseteq A$, $A \in \mathcal{A}$, $X \in F(A)$, then either (i) F is everywhere tangent to S or (ii) F is nowhere tangent to S. ($\mathcal{S}$ is compatible with $\mathcal{A}$ is every set in $\mathcal{A}$ is a union of sets in $\mathcal{S}$.)*

Theorem 4.5 is illustrated by the following example.

Example 4.6. Let F be the following analytic vector field on $\mathbb{R}^2$

$$\begin{aligned} \dot{x} &= x^2 + y^2 \\ \dot{y} &= 0 \end{aligned}$$

which has an isolated equilibrium at the origin and points in the positive x-direction otherwise. Consider the following two subanalytic sets

$$\begin{aligned} S_1 &= \{(x,y) \in \mathbb{R}^2 \mid y \geq 0 \quad \text{and} \quad (x-1)^2 + y^2 = 1\} \\ S_2 &= \{(x,y) \in \mathbb{R}^2 \mid y = 0 \quad \text{and} \quad 0 \leq x \leq 2\} \end{aligned}$$

shown in Figure 3. A subanalytic stratification of $\mathbb{R}^2$ which is compatible with the sets S_1, S_2 and the vector field F is also shown in Figure 3. It consists of

- 0-dimensional strata
  - $P_1 = (0,0)$, $P_2 = (2,0)$, and $P_3 = (1,1)$
- 1-dimensional strata
  - $C_1 = \{(x,y) \in \mathbb{R}^2 \mid y = 0 \quad \text{and} \quad 0 < x < 2\}$
  - $C_2 = \{(x,y) \in \mathbb{R}^2 \mid y > 0 \quad \text{and} \quad 1 < x < 2 \quad \text{and} \quad (x-1)^2 + y^2 = 1\}$
  - $C_3 = \{(x,y) \in \mathbb{R}^2 \mid y > 0 \quad \text{and} \quad 0 < x < 1 \quad \text{and} \quad (x-1)^2 + y^2 = 1\}$
- 2-dimensional strata
  - $D_1 = \{(x,y) \in \mathbb{R}^2 \mid y > 0 \quad \text{and} \quad (x-1)^2 + y^2 < 1\}$
  - $D_2 = \mathbb{R}^2 \setminus \{P_1, P_2, P_3, C_1, C_2, C_3, D_1\}$

Notice that the vector field is tangent to P_1 since it is an equilibrium as well as to C_1, D_1 and D_2. The vector field is transverse to all the other strata. Moreover, $S_1 = P_1 \cup P_2 \cup P_3 \cup C_2 \cup C_3$ and $S_2 = P_1 \cup P_2 \cup C_1$.

In view of the above properties we will restrict our study to hybrid systems for which the relevant sets are all relatively compact and subanalytic.

Assumption 1 : For each discrete state q the collection $\mathcal{A}_q$ consists of relatively compact subanalytic sets. In particular, we assume there exists a compact set K such that if $A \in \mathcal{A}_q$ then $A \subseteq K$.

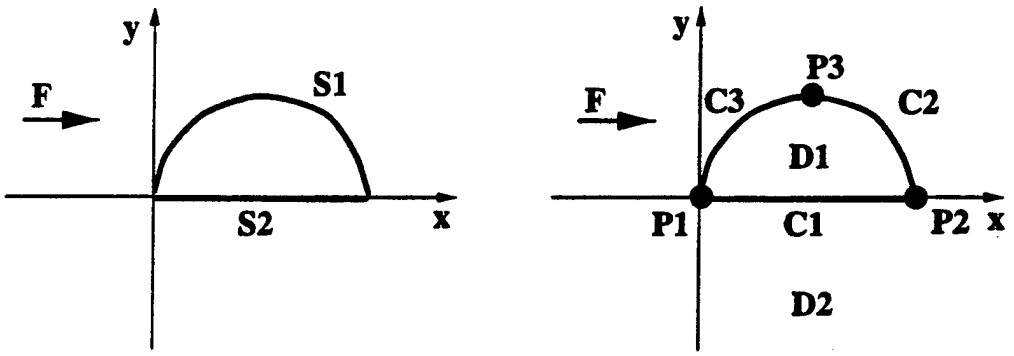

FIGURE 3. Subanalytic stratification example

The partition $\mathcal{S}_q$ which serves as the initialization step of **Algorithm 2** can now be assumed to be a subanalytic stratification compatible with $\mathcal{A}_q$ and the vector field $F(q,\cdot)$ (as given by Theorem 4.5).

The following proposition illustrates some of the good intersection properties that analytic curves have with subanalytic sets. The "finiteness" property indicated in the proposition makes it possible to define transitions between adjacent strata in a natural way.

Proposition 4.7. *Let I be an open interval, M a real analytic manifold and $\gamma\colon I \to M$ a real analytic function. Let $\mathcal{S}$ be a C^ω stratification of M by subanalytic sets If $[a,b] \subset I$ then there exists a finite partition $\{x_1,\ldots,x_n\}$ of $[a,b]$ with the property that for each $i = 1,\ldots,n-1$ there exists a stratum $S_i \in \mathcal{S}$ such that $\gamma((x_i,x_{i+1})) \subseteq S_i$.*

Proof. The family $\mathcal{I} = \{\gamma^{-1}(S) \cap [a,b]\colon S \in \mathcal{S}\}$ is a finite partition of $[a,b]$ by subanalytic sets. Each such set consists of a finite number of points and open intervals. Using all such points and the endpoints of such intervals gives the desired partition. □

The following example shows the type of pathological situations that can be encountered if the assumption on subanalyticity is even slightly relaxed.

Example 4.8. Consider the stratification of $\mathbb{R}^2$ by the following five sets:

$$
\begin{aligned}
S_1 &= \{(0,0)\} \\
S_2 &= \left\{(x,y)\colon x>0 \wedge y = x\sin\frac{1}{x}\right\} \\
S_3 &= \left\{(x,y)\colon x<0 \wedge y = x\sin\frac{1}{x}\right\} \\
S_4 &= \left\{(x,y)\colon x\neq 0 \wedge y > x\sin\frac{1}{x}\right\} \bigcup \{(0,y)\colon y>0\} \\
S_5 &= \left\{(x,y)\colon x\neq 0 \wedge y < x\sin\frac{1}{x}\right\} \bigcup \{(0,y)\colon y<0\}
\end{aligned}
$$

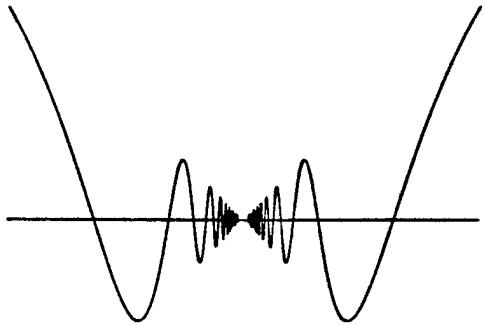

FIGURE 4. Infinite crossings on a compact interval

Notice that S_1, S_2 and S_3 form the graph of the function $f(x) = x \sin \frac{1}{x}$ ($f(0) = 0$), while S_4 and S_5 denote the region above and the below the graph, respectively. Each set is a C^ω, embedded submanifold of $\mathbb{R}^2$ and they clearly satisfy the condition on the dimension of the strata in the closure of other strata. Finally, consider the constant vector field $F = \frac{\partial}{\partial x}$. Then the integral curve γ of F through $(0,0)$ is the x-axis (parameterized by x itself). Therefore, the image by γ of any interval containing 0 intersects both S_4 and S_5 an infinite number of times. This is reminiscent of the undesirable zeno property which allows an infinite number of switches in finite time.

Since the algorithm considers one discrete state at a time, we will simplify the notation by assuming that the discrete state q is fixed and drop it as a subscript. In particular we will consider a vector field F and a stratification $\mathcal{S}$ of X_C by subanalytic sets as provided by Theorem 4.5. By $X_C/\sim$ we will mean the partition of X_C induced by $\mathcal{S}$. We will denote by γ_x the integral curve of F which passes through x at time 0, i.e. with $\gamma_x(0) = x$.

We now proceed to formalize the notion of a discretization of the continuous transitions relative to a given partition $\mathcal{S}$. We do this mainly it simplifies the arguments in the proof of the main theorem (Theorem 6.1). In addition it supports the intuitive picture we have that a trajectory can be decomposed as a concatenation of pieces in each of the sets in $\mathcal{S}$.

Definition 4.9 (Transition relative to $\mathcal{S}$: version 1). Given $x, y \in X_C$ we say $x \xrightarrow{\mathcal{S}} y$ iff there is $t > 0$ such that $\gamma_x(t) = y$ and there exists $S \in \mathcal{S}$ such that $\gamma_x(s) \in S$ for $0 < s < t$ and at least one of x, y is in S.

To clarify this concept and to facilitate further discussions and proofs we introduce additional definitions.

Definition 4.10. Given two subsets S_1, S_2 of X_C, and a real analytic curve $\gamma : I \to X_C$ where I is an open interval, we say that γ *leaves* S_1 *through* S_2 (or *enters* S_2 *from* S_1) if one of the following exiting conditions is satisfied:

E1: there exist $a, b \in I$, $a < b$, such that $\gamma(t) \in S_1$ for all $t \in (a, b)$ and $\gamma(b) \in S_2$
E2: there exist $a, b \in I$, $a < b$, such that $\gamma(a) \in S_1$ and $\gamma(t) \in S_2$ for all $t \in (a, b)$.

When $x \in S_1$ we say that γ_x leaves S_1 trough S_2 if either **E1** or **E2** holds with $a = 0$.

The following proposition is a simple application of Proposition 4.7 and shows that Definition 4.10 covers all possible "exiting" situations for strata of $\mathcal{S}$.

Proposition 4.11. *Let $S_1 \in \mathcal{S}$ and γ be as above. If there exists $t_0, t_1 \in I$ such that $\gamma(t_0) \in S_1$ and $\gamma(t_1) \notin S_1$ then there exists a stratum S_2 ($\neq S_1$) such that either* **E1** *or* **E2** *holds.*

It is clear from Definition 4.10 that in case **E1**, $S_2 \cap \overline{S}_1 \neq \emptyset$. By the properties of stratifications, we conclude $S_2 \subset \overline{S}_1$ and $\dim S_2 < \dim S_1$. Therefore, the flow exits the stratum S_1 though a stratum of lower dimension. Similarly in case **E2**, $S_1 \subset \overline{S}_2$ and $\dim S_1 < \dim S_2$ and the flow enters S_2 from a stratum of lower dimension. The following proposition further clarifies the possible exit situations.

Definition 4.12. We call a stratum $S \in \mathcal{S}$ *tangential* if the vector field F is tangent to S at every point of S. We call a stratum *transversal* otherwise.

Proposition 4.13. *Let S_1, S_2 be strata in $\mathcal{S}$ and γ an integral curve of F which leaves S_1 through S_2. Then one (and only one) of the following holds:*

1. *condition* **E1** *holds, S_1 is a tangential stratum and S_2 is a transversal stratum.*
2. *condition* **E2** *holds, S_1 is a transversal stratum and S_2 is a tangential stratum.*

We can now give the alternative definition of relative transitions.

Definition 4.14 (Transition relative to $\mathcal{S}$: version 2). For each $x \in X_C$ let $S(x)$ denote the unique stratum in $\mathcal{S}$ which contains x. Given $x, y \in X_C$ we say $x \xrightarrow{\mathcal{S}} y$ iff γ_x leaves $S(x)$ through $S(y)$.

It is clear from Proposition 4.7 that $x \xrightarrow{\tau} y$ iff there exist $x_1, \ldots, x_n$ such that $x \xrightarrow{\mathcal{S}} x_1 \xrightarrow{\mathcal{S}} \ldots \xrightarrow{\mathcal{S}} x_n \xrightarrow{\mathcal{S}} y$. We will denote the *Pre* operator associated to $\xrightarrow{\mathcal{S}}$ by $Pre_{\mathcal{S}}$. The above remark also implies that we can substitute $Pre_{\mathcal{S}}$ for Pre_τ in **Algorithm 2** in the sense that if the algorithm terminates using $Pre_{\mathcal{S}}$ then it also terminates when using Pre_τ.

As the stratification Theorem 4.5 shows, issues of transversality of trajectories can be analyzed within the context of subanalytic sets and analytic vector fields. However, the study of continuous transitions requires that we investigate the global behavior of trajectories. In general, trajectories of analytic vector fields (and much less their full flows) are not subanalytic. Identifying vector fields whose flows belong to a suitable class is the main obstacle in the study of bisimulations of hybrid systems. Recent developments in logic model theory provide some answers as well as suggest the proper context in which to carry on further studies.

5. Model Theory

Model theory studies structures through properties of their definable sets (see [14, 25] for general background). The basic structures of interest for this paper are that of the real numbers as a complete ordered field, symbolized by $(\mathbb{R}, +, -, \times, <, 0, 1)$, and its extensions. Every such

structure L has an associated language $\mathcal{L}$ of formulas. The (first order) formulas over $\mathcal{L}$ are the well-formed logical expressions obtained by using logical connectives, quantifiers $\exists\ \forall$, real numbers as constants, the operations of additions and multiplication, and the relations $<$ and $=$ (quantification is allowed over variables). All formulas will be interpreted over the real numbers. A *definable set* in the language $\mathcal{L}$ (or of the structure L) is a subset of $\mathbf{R}^n$ (for some n) of the form $\{(a_1,\ldots,a_n) \in \mathbf{R}^n : \Phi(a_1,\ldots,a_n)\}$, where $\Phi(x_1,\ldots,x_n)$ is a formula in $\mathcal{L}$ and $x_1,\ldots,x_n$ are free (i.e. not quantified) variables in Φ. A function f is definable if its graph is a definable set.

While many of the concepts here apply to more general structures, in all that follows we consider only structures over the real numbers.

Definition 5.1. The theory of $\mathcal{L}$ is *o-minimal* ("order minimal") if every definable subset of $\mathbb{R}$ is a finite union of points and intervals (possibly unbounded).

Tarski [24] was interested in the extension of the theory of the real numbers by the exponential function, $(\mathbb{R}, +, -, \times, <, 0, 1, \exp)$ (i.e., there is an additional symbol in the language for the exponential function). We denote this structure by $\mathbb{R}_{\exp}$. While such theory does not admit elimination of quantifiers, it was shown in [27] that such theory is model complete, which in turns implies that it is o-minimal. Another important extension is obtained as follows. Assume f is a real-analytic function in a neighborhood of the cube $[-1,1]^n \subset \mathbb{R}^n$. Let $\hat{f}\colon \mathbb{R}^n \to \mathbb{R}$ be the function defined by

$$\hat{f}(x) = \begin{cases} f(x) & \text{if } x \in [-1,1]^n \\ 0 & \text{otherwise} \end{cases}$$

We call such functions *restricted analytic functions.* The structure $\mathbb{R}_{\exp,\mathrm{an}} = (\mathbb{R}, +, -, \times, <, 0, 1, \exp, \{\hat{f}\})$ is then an extension of $\mathbb{R}_{\exp}$ where there is a symbol for each restricted analytic function. One reason this structure is relevant for this paper is that all relatively compact subanalytic sets are definable in $\mathbb{R}_{\exp,\mathrm{an}}$. Moreover, if F is a linear vector field in $\mathbb{R}^n$ with real eigenvalues, then the trajectories of F are definable in $\mathbb{R}_{\exp,\mathrm{an}}$. In [26], it was shown that $\mathbb{R}_{\exp.\mathrm{an}}$ is also o-minimal. Finally, there are a few consequences of o-minimality that are crucial for our results. We list them below under one proposition. The proofs are contained in the various references mentioned above.

Proposition 5.2. *Assume L is an o-minimal structure. Then*

1. *Any definable set has a finite number of connected components, each of which is a definable set.*
2. *If A is definable, then so is its (topological) closure. Moreover,* $\dim Fr(A) < \dim A$, *where $Fr(A) = \overline{A} \setminus A$ is the frontier of A and the dimension of a set $B \subset \mathbf{R}^n$ is the maximum integer d for which there is an embedded C^1 manifold of $\mathbf{R}^n$ contained in B.*
3. *Given definable sets $A_1,\ldots,A_k$ in $\mathbf{R}^n$ (and for any integer p), there is a finite C^p stratification of $\mathbf{R}^n$ compatible with $\{A_1,\ldots,A_k\}$. In fact, for the structure $\mathbb{R}_{\exp,\mathrm{an}}$ the strata are definable (real) analytic manifolds.*

We are now ready to apply these results to prove that **Algorithm 2** terminates for certain classes of planar systems.

6. Finiteness Results

In this section we use the model theoretic tools of Section 5 in order to obtain classes of systems for which the Bisimulation Algorithm of Section 3 terminates.

Recall that given the family of sets $\mathcal{A}$ as in Assumption 1, and the vector field F we first obtain a stratification $\mathcal{S}$ compatible with $\mathcal{A}$ as given by Theorem 4.5. We will also assume that $\mathcal{S}$ is compatible with a compact subanalytic set K which contains all sets in $\mathcal{A}$. We define $\mathcal{S}_K = \{S \in \mathcal{S} : S \cap K \neq \emptyset\}$ (which is therefore finite).

Theorem 6.1. *Let $X_C = \mathbb{R}^2$, F be the linear vector field Ax and assume that the eigenvalues of A are real. Then the bisimulation algorithm for hybrid systems (**Algorithm 2**), initialized with $\mathcal{S}_K$, terminates.*

Proof. We will consider the case when the origin is the only equilibrium of F. (The other cases require minor modifications.) We assume without loss of generality that $\{(0,0)\} \in \mathcal{S}_K$.

As indicated in Section 3 it suffices to study only the evolution of the continuous variables and use $Pre_{\mathcal{S}}$ in **Algorithm 2**. To simplify notation we will simply refer to it as Pre. In order to show that the bisimulation algorithm terminates we will construct a finite refinement of $\mathcal{S}_K$ which is "invariant" under the Pre operation and which is a refinement of $X_C/\sim$ at each step.

For each stratum $S \in \mathcal{S}_K$ with $(0,0) \in \overline{S}$ we consider the set

$$S_\infty = \{x \in S : \forall\, t \geq 0 \;\; \gamma_x(t) \in S\}$$

As mentioned earlier, since the eigenvalues of A are real, the flow of F, $\Phi(x,t) = \gamma_x(t) = e^{tA}x$ is definable in $\mathbb{R}_{\exp,an}$ (the entries in e^{tA} involve polynomials and real exponential functions). Therefore, the set S_∞ is definable. For each stratum T of dimension one with $T \subset \overline{S}$, $T \neq S$, we consider the set

$$T_* = \{x \in T : \gamma_x \text{ leaves } T \text{ through } S_\infty\}$$

The set T_* is also definable in $\mathbb{R}_{\exp,an}$ and therefore can be written as a finite, disjoint union of definable sets each of which is either a point or homeomorphic to an open interval. We may assume, by refining the original $\mathcal{S}_K$ if necessary that the finitely many points in the decomposition of T_* are already strata of $\mathcal{S}_K$.

For each $x \in \mathbb{R}^2$ let Γ_x denote the trajectory of F passing through x, that is

$$\Gamma_x = \{\gamma_x(t) : t \in \mathbf{R}\}.$$

For each stratum $S \in \mathcal{S}$ and $x \in S$, let $\Gamma_x(S)$ denote the connected component of $\Gamma_x \cap S$ which contains x. It is clear, from the definition of S_∞, that if $x \in S_\infty$ then $\Gamma_x(S) \subset S_\infty$. From this it follows that if $x \in T$ and γ_x leaves T through S then γ_x either leaves T though S_∞ or leaves T through $S \setminus S_\infty$.

Let $\{p_1\}, \ldots, \{p_l\}$ be all the 0-dimensional strata of $\mathcal{S}_K$. Notice that for each i, j, if $\Gamma_{p_i} \cap \Gamma_{p_j} \neq \emptyset$, then $\Gamma_{p_i} = \Gamma_{p_j}$. We will eliminate redundancies and assume that the Γ_{p_i} are pairwise disjoint. For each set $S \in \mathcal{S}_K$ and each Γ_{p_i}, the sets $S \cap \Gamma_{p_i}$ and $S \setminus \cup_i \Gamma_{p_i}$ are definable in

$\mathbb{R}_{\exp,an}$ (Intuitively, these sets are partitions of S "in the direction of the flow of F"). By o-minimality, we get that each such set has a finite number of connected components. Let $\mathcal{B}$ denote the (finite) collection of all such connected components. The collection $\mathcal{B}$ is then a partition of K compatible with $\mathcal{S}$ (every set in $\mathcal{S}$ is a union of sets in $\mathcal{B}$).

Claim: At each step of the bisimulation algorithm, $\mathcal{B}$ is compatible with $M/\sim$.

The claim shows that $\mathcal{B}$ is finer than all partitions obtained at each step. Since $\mathcal{B}$ is finite, this proves that the algorithm terminates.

To prove the claim we first show that if $B_i \in \mathcal{B}$ for $i = 1, \ldots, n$ then

$$Pre(\cup B_i) = \cup Pre(B_i) \tag{6.1}$$

We will call a set $B \in \mathcal{B}$ tangential if B is contained in a tangential stratum of $\mathcal{S}$ (i.e. B is a connected component of either $S \cap \Gamma_q$ or $S \setminus \cup \Gamma_{p_i}$ with S tangential). The set B will be called transversal otherwise. Notice that if B is tangential and $x \in B$ then $\Gamma_x(S(x)) \subset B$.

Let $x \in Pre(B_i)$ for some $i = 1, \ldots, n$ and $x \notin B_i$. Suppose $\gamma_x(t) \in S(x)$ for $0 \leq t < \delta$ and $\gamma_x(\delta) \in B_i$ (i.e. exit condition **E1**). In particular, $S(x)$ is a tangential stratum. If $\gamma_x(t) \notin \cup B_i$ for $t < \delta$, then $x \in Pre(\cup B_i)$. If $\gamma_x(t) \in \cup B_i$ for some $t < \delta$, then for some j, B_j is tangential, so $\Gamma_x(S(x)) \subset B_j$ and $x \in Pre(\cup B_i)$. If, instead, $\gamma_x(t) \in B_i$ for $0 < t < \delta$ (exit condition **E2**), then clearly $x \in Pre(\cup B_i)$.

Conversely, let $x \in Pre(\cup B_i)$. If $\gamma_x(t) \in S(x)$ for $0 \leq t < \delta$, $\gamma_x(\delta) \in \cup B_i$, let i_0 be such that $\gamma_x(\delta) \in B_{i_0}$. Then $x \in Pre(B_{i_0}) \subset \cup Pre(B_i)$. If, instead, $\gamma_x(t) \in \cup B_i$ for $0 < t < \delta$, then there is a $\delta_0 > 0$ and a B_{i_0} which contains $\gamma_x(t)$ for $0 < t < \delta_0$ (here we used o-minimality again to conclude that Γ_x intersects each B_i in a finite disjoint union of points and arcs). Therefore, $x \in Pre(B_{i_0})$. This conclude the proof of (6.1).

By construction, $\mathcal{B}$ is compatible with $\mathcal{S}_K$. At each step of the bisimulation algorithm we need to show that if $B = \cup_{i=1}^n B_i$ and $B' = \cup_{j=1}^m B'_i$ with $B_i, B'_i \in \mathcal{B}$ then $B \cap Pre(B')$ is again a finite union of sets in $\mathcal{B}$. Based on (6.1) it will suffice to show that for $B, B' \in \mathcal{B}$, either $B \cap Pre(B') = \emptyset$ or $B \cap Pre(B') = B$.

We consider several cases. The set B is of one of the two forms: (a) a connected component of $S \cap \Gamma_{p_i}$, or (b) a connected component of $S \setminus \cup \Gamma_{p_i}$.

If S is 0-dimensional there is nothing to show because B contains a single point.

If S is 1-dimensional and B is of type (a), then either S is transversal and B consists of a single point or S is tangential and so $B = \Gamma_x(S)$ for any $x \in B$. The first case is again clear. In the second case, if there is $x \in B \cap Pre(B')$ then there exists $\delta > 0$ such that $\gamma_x(t) \in S$ for $0 \leq t < \delta$ and $\gamma_x(\delta) \in B'$. But then for all $y \in \Gamma_x(S)$, γ_y leaves S through B'. So $B = \Gamma_x(S) \subset Pre(B')$.

If S is 1-dimensional and B is of type (b) then we again consider separately the cases when S is tangential and when S is transversal. In the first case we proceed as before. Assume now, that S is transversal. Notice that if $x \in B \cap Pre(B')$ then Γ_x intersects both B and B'. Therefore B' is also a connected component of $S' \setminus \cup \Gamma_{p_i}$ (for some S'). By transversality, γ_x leaves S intro S' under exit condition **E2** and so $S \subset Fron(S')$ $(= \overline{S'} \setminus S')$ and S' is

2-dimensional. By continuity of the flow of F, there is an open neighborhood N of x such that for $y \in N \cap B$, γ_y leaves S through S'. Moreover, since there are finitely many Γ_{p_i} we may assume (by taking N smaller) that γ_y leaves S through B'. We have then showed that the set $E = \{x \in B : \gamma_x$ leaves S through $B'\}$ is open in B. Suppose $E \neq B$. Then there is $y \in B$ in the frontier of E. We can find a neighborhood W of y such that $W \cap \Gamma_{p_i} = \emptyset$ for all i. Since S' is open in $\mathbb{R}^2$, and S is transversal, we can find a neighborhood $W_0 \subset W$ of y and $\varepsilon > 0$ such that for $z \in W_0 \cap S$ and $0 < t < \varepsilon$ we have $\gamma_x(t) \in W \cap S'$. But then every such z belongs to E. This contradicts the fact that y is a frontier point. Therefore, E is also closed in B and so it must equal B (since B is connected). We conclude in this case that $B = B \cap Pre(B')$.

There is only one case remaining: S of dimension 2 (and hence tangential). If B is of type (a) then $\Gamma_x(S) = B$ and we are done as before.

Assume then that B is a connected component of $S \setminus \cup\Gamma_{p_i}$, B' a connected component of $S' \setminus \cup\Gamma_{p_i}$, S' is transversal, and $\dim S' = 1$. (The case with S' 0-dimensional is excluded since in that case $S' \cap \Gamma_{p_i} \neq \emptyset$ for some i.)

Let $x \in B \cap Pre(B')$ and assume there is $y \in B \setminus Pre(B')$. We want to show that this leads to a contradiction. Let $\alpha : [0,1] \to B$ be a curve connecting x to y. Let t_0 be the smallest $t \in [0,1]$ such that $\gamma_{\alpha(t)}(s) \notin B'$ for some $s > 0$. If $\gamma_{\alpha(t_0)}(s) \in S$ for all $s > 0$ then $\alpha(t_0) \in S_\infty$. By the choice of t_0 we in fact have $\alpha(t_0) \in \Gamma_{p_0}$ for some p_0 (see the initial subdivision caused by S_∞). But this contradicts the fact that B is of type (b). Assume then that $\gamma_{\alpha(t_0)}(s) \notin S$ for some $s > 0$. For each $t \in [0, t_0]$ let $s(t)$ be the smallest s such that $\gamma_{\alpha(t)}(s) \notin S$. For each $t \in [0, t_0]$ set $p(t) = \gamma_{\alpha(t)}(s(t))$. There are two possibilities: either $p(t_0) \in S'$ or $p(t_0) \in \overline{S'} \setminus S$.

In the first case choose a local chart (N, φ) centered at $p(t_0)$ so that in φ-coordinates we have $N \cap S' = N \cap B' = \{(x, 0)\}$ and $N \cap S = \{(x, y) : y > 0\}$ (therefore F points into the lower half plane at every point of $N \cap B'$. By continuity of the flow and transversality, we still have that $\gamma_{\alpha(t)}$ crosses $N \cap B'$ from the upper to the lower half plane for $t_0 < t < t_0 + \epsilon$. But this contradicts the choice of t_0.

In the second case, we have $p(t_0) \in \Gamma_{q_0}$ for some q_0. But this contradicts the fact that B is of type (b).

All this implies that every y in B must also be in $Pre(B')$. That is, $B = B \cap Pre(B')$. This concludes the proofs of the claim and the theorem. □

As the proof above suggests the termination of the algorithm depends on the fact that the integral curves of the vector field intersects relatively compact subanalytic sets in at most finitely many points. This allows us to get the following generalization.

Theorem 6.2. *If F is an analytic vector field in $\mathbb{R}^2$ which admits an analytic family of first integrals, then the bisimulation algorithm terminates. (Here, by an analytic family of first integrals we mean a non-constant (real) analytic function $f: \mathbb{R}^2 \to \mathbb{R}$ such that for each trajectory γ of F the function $f(\gamma(t))$ is constant.)*

Proof. Notice that each level curve of f is an analytic set and therefore its intersection with any relatively compact definable set (in $\mathbb{R}_{\exp,an}$) is definable in $\mathbb{R}_{\exp,an}$. The proof then follows the lines of the previous one but replacing the sets Γ_{p_i}, with the corresponding level set of f (level sets of f are at most 1-dimensional since f is not constant on any open set). □

Corollary 6.3. *If F is a linear vector field in $\mathbb{R}^2$ with purely imaginary eigenvalues and S_K is as in the theorem, then the bisimulation algorithm terminates.*

Proof. Unless $A = 0$, in which case the result is trivial, there exists an (invertible) matrix P such that $\|Px\|^2$ is constant along trajectories of F. □

Corollary 6.4. *If F is an analytic Hamiltonian vector field in $\mathbb{R}^2$ and S_K is as above, then the bisimulation algorithm terminates.*

Proof. The Hamiltonian is constant along the trajectories. □

Remark 6.5. As is clear from the proofs above, the key is that all the objects involved (the vector field F, the initial family of sets, the flow of F) be definable in some o-minimal extension of the field of real numbers. We presented above just two specific instances of such a situation which can be easily characterized. A more recent o-minimal extension of the reals, by so called Pfaffian functions, was found in [28].

The issue of decidability is a much harder and still open problem. It is not even known if the theory of $\mathbb{R}_{\exp}$ is decidable, although in [15] it was shown that it would be a consequence of Schanuel's conjecture in number theory. The results we obtained in this paper suggest how to find some restricted classes of vector fields for which the algorithm is constructive. Indeed, if all the relevant sets are semialgebraic (for example if F is a Hamiltonian vector field on the plane with a polynomial Hamiltonian and the initial conditions, guards, etc., are semialgebraic), then they are definable in $(\mathbb{R}, +, -, \times, <, 0, 1)$ for which decision methods are known (see [9] for a related result).

7. Conclusions

In this paper, we presented an algorithm for on obtaining finite bisimulations of hybrid systems. Termination was guaranteed for classes of vector fields with planar continuous dynamics. This was achieved by combining the geometric framework of subanalytic sets with model theoretic concepts from mathematical logic. The mathematical tools used in this paper provide the natural platform for the study of reachability properties of hybrid systems.

Issues for further study include the extension of the main result to $\mathbb{R}^n$. The tools used in the proof of the main theorem apply to higher dimensions. The key construction in the two dimensional case depended on finitely many trajectories. The higher dimensional version requires a detailed analysis of infinite collections of trajectories, organized perhaps inductively according to the dimension of the strata involved.

Bisimulations of hybrid systems with more general discrete transitions can also be considered in the framework of subanalytic stratifications and o-minimal structures. However,the reset

maps must be in some sense compatible with the flows for the procedure to terminate. In addition, for certain restricted classes of vector fields the algorithm can be made constructive (for example, for vector fields on the plane with a polynomial Hamiltonian and all relevant sets semialgebraic). Furthermore, if the bisimulation algorithm does not terminate (or is not computable), it may be useful to consider system over-approximations [19], for which the algorithm would terminate (or is computable).

Acknowledgment: This research is supported by the Army Research Office under grants DAAH 04-95-1-0588 and DAAH 04-96-1-0341.

REFERENCES

[1] R. Alur and D.L. Dill. A theory of timed automata. *Theoretical Computer Science*, 126:183–235, 1994.

[2] R. Alur, T.A. Henzinger, and E.D. Sontag, editors. *Hybrid Systems III*, volume 1066 of *Lecture Notes in Computer Science*. Springer-Verlag, 1996.

[3] P. Antsaklis, W. Kohn, A. Nerode, and S. Sastry, editors. *Hybrid Systems II*, volume 999 of *Lecture Notes in Computer Science*. Springer-Verlag, 1995.

[4] P Antsaklis, W. Kohn, A. Nerode, and S. Sastry, editors. *Hybrid Systems IV*, volume 1273 of *Lecture Notes in Computer Science*. Springer-Verlag, 1997.

[5] P.J. Antsaklis, J.A. Stiver, and M. Lemmon. Hybrid system modeling and autonomous control systems. In R. L. Grossman, A. Nerode, A. P. Ravn, and H. Rischel, editors, *Hybrid Systems*, volume 736 of *Lecture Notes in Computer Science*, pages 366–392. Springer-Verlag, 1993.

[6] Edward Bierstone and Pierre D. Milman. Semianalytic and subanalytic sets. *Inst. Hautes Études Sci. Publ. Math.*, 67:5–42, 1988.

[7] P.E. Caines and Y.J. Wei. The hierarchical lattices of a finite state machine. *Systems and Control Letters*, 25:257–263, 1995.

[8] P.E. Caines and Y.J. Wei. Hierarchical hybrid control systems: A lattice theoretic formulation. *IEEE Transactions on Automatic Control : Special Issue on Hybrid Systems*, 43(4), April 1998.

[9] Karlis Cerans and Juris Viksna. Deciding reachability for planar multi-polynomial systems. In R. Alur, T. Henzinger, and E.D. Sontag, editors, *Hybrid Systems III*, volume 1066 of *Lecture Notes in Computer Science*, pages 389–400. Springer Verlag, Berlin, Germany, 1996.

[10] R. L. Grossman, A. Nerode, A. P. Ravn, and H. Rischel, editors. *Hybrid Systems*, volume 736 of *Lecture Notes in Computer Science*. Springer-Verlag, 1993.

[11] T.A. Henzinger. Hybrid automata with finite bisimulations. In Z. Fülöp and F. Gécseg, editors, *ICALP 95: Automata, Languages, and Programming*, pages 324–335. Springer-Verlag, 1995.

[12] T.A. Henzinger, P.W. Kopke, A. Puri, and P. Varaiya. What's decidable about hybrid automata? In *Proceedings of the 27th Annual Symposium on Theory of Computing*, pages 373–382. ACM Press, 1995.

[13] H. Hironaka. Subanalytic sets. In *In Number Theory, Algebraic Geometry, and Commutative Algebra, in honor of Y. Akizuki*, pages 453–493. Kinokuniya Publications, 1973.

[14] W. Hodges. *A Shorter Model Theory*. Cambridge University Press, 1997.

[15] A. Macintyre and A.J. Wilkie. On the decidability of the real exponential field. In *Kreiseliana: About and around Georg Kreisel*, pages 441–467. A.K. Peters, 1996.

[16] O. Maler, editor. *Hybrid and Real-Time Systems*, volume 1201 of *Lecture Notes in Computer Science*. Springer-Verlag, 1997.

[17] T. Niinomi, B.H. Krogh, and J.E.R. Cury. Synthesis of supervisory controllers for hybrid systems based on approximating automata. In *Proceedings of the 1995 IEEE Conference on Decision and Control*, pages 1461–1466, New Orleans, LA, December 1995.

[18] George J. Pappas, Gerardo Lafferriere, and Shankar Sastry. Hierarchically consistent control systems. In *Proceedings of the 37th IEEE Conference in Decision and Control*. Tampa, FL, December 1998. Submitted.

[19] George J. Pappas and Shankar Sastry. Towards continuous abstractions of dynamical and control systems. In P. Antsaklis, W. Kohn, A. Nerode, and S. Sastry, editors, *Hybrid Systems IV*, volume 1273 of *Lecture Notes in Computer Science*, pages 329–341. Springer Verlag, Berlin, Germany, 1997.

[20] Anuj Puri and Pravin Varaiya. Decidability of hybrid systems with rectangular differential inclusions. In *Computer Aided Verification*, pages 95–104, 1994.

[21] J. Raisch and S.D. O'Young. Discrete approximations and supervisory control of continuous systems. *IEEE Transactions on Automatic Control : Special Issue on Hybrid Systems*, 43:4, April 1998. To appear.

[22] Héctor J. Sussmann. Subanalytic sets and feedback control. *Journal of Differential Equations*, 31(1):31–52, January 1979.

[23] Héctor J. Sussmann. Real-analytic desingularization and subanalytic sets: An elementary approach. *Transactions of the American Mathematical Society*, 317(2):417–461, February 1990.

[24] Alfred Tarski. *A decision method for elementary algebra and geometry.* University of California Press, second edition, 1951.

[25] Dirk van Dalen. *Logic and Structure.* Springer-Verlag, third edition, 1994.

[26] Lou van den Dries and Chris Miller. On the real exponential field with restricted analytic functions. *Israel Journal of Mathematics*, 85:19–56, 1994.

[27] A. J. Wilkie. Model completeness results for expansions of the ordered field of real numbers by restricted pfaffian functions and the exponential function. *Journal of the AMS*, 9(4):1051–1094, Oct 1996.

[28] A.J. Wilkie. A general theorem of the complement and some new o-minimal structures. Preprint, 1997.

DEPARTMENT OF MATHEMATICAL SCIENCES, PORTLAND STATE UNIVERSITY, PORTLAND, OR 97207

E-mail address: gerardo@mth.pdx.edu

DEPARTMENT OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCES, UNIVERSITY OF CALIFORNIA AT BERKELEY, BERKELEY, CA 94720

E-mail address: gpappas@eecs.berkeley.edu

DEPARTMENT OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCES, UNIVERSITY OF CALIFORNIA AT BERKELEY, BERKELEY, CA 94720

E-mail address: sastry@eecs.berkeley.edu